Ms. Věra Jourová
Commissioner for Justice, Consumers and Gender Equality
European Commission
Rue de la Loi / Wetstraat 200
1049 Brussels
Belgium

July 26, 2017

Dear Commissioner Jourová:

Human Rights Watch and Amnesty International write to urge the European Commission to re-evaluate its *Implementing Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield* on the basis that the United States of America (United States) does not ensure a level of fundamental rights protection regarding the processing of personal data that is essentially equivalent to that guaranteed within the European Union (EU).

We further call on the European Commission to encourage the US legislative and executive branches to adopt the necessary binding reforms so that the transfer of personal data to the United States does comply with the requirements of the Charter of Fundamental Rights of the EU, the Data Protection Directive, and the General Data Protection Regulation.

We believe the Commission's conclusions regarding the adequacy of rights protections afforded by the US are incorrect because, among other reasons, the country's two main foreign intelligence surveillance laws—and the programs that are avowedly or reportedly conducted under them—demonstrably fall far short of essential equivalence to the standards set out in EU law and do not comport with international human rights guarantees. We are also concerned about the lack of safeguards applicable to US intelligence-sharing arrangements with other states and of effective remedies for fundamental rights violations stemming from intelligence surveillance activities.

In the enclosed briefing, you will find our detailed assessment of US legal authorities and surveillance activities and our conclusions regarding why they fail to provide an adequate level of protection for the purposes of EU law.

An earlier joint letter from Human Rights Watch and the American Civil Liberties Union has addressed separate concerns about the weakening of Privacy Act protections for EU nationals

and other non-US citizens as well as the current inability of the Privacy and Civil Liberties Oversight Board to function.[1]

Thank you in advance for your engagement and we stand ready to provide any further information you may require.

Yours sincerely,

Maria McFarland Sánchez-Moreno
Co-Director, US Program
Human Rights Watch

Iverna McGowan
Head of European Institutions Office and Advocacy Director
Amnesty International

Annex: Assessment of the Adequacy of US Surveillance Laws and Practices for the Purposes of EU Law

CC:

- Ms. Renate Nikolay, Head of Cabinet, European Commission
- Mr. Kevin O'Connell, Member of Cabinet, European Commission
- Mr. Bruno Gencarelli, Head of Unit, Directorate-General Justice and Consumers, European Commission
- H.E. David O'Sullivan, Ambassador/Head of Delegation, European Union Delegation to the United States
- Mr. Aymeric Dupont, Counselor for Justice and Home Affairs, European Union Delegation to the United States
- Ms. Monika Maglione, Counselor for Justice and Home Affairs, European Union Delegation to the United States
- Mr. Andrea Glorioso, Counselor for the Digital Economy, European Union Delegation to the United States

[1] American Civil Liberties Union & Human Rights Watch, Letter to Věra Jourová, Feb. 28, 2017, available at https://www.hrw.org/news/2017/02/28/joint-letter-commissioner-jourova-re-privacy-shield.

Human Rights Watch and Amnesty International Briefing:

Assessment of the Compliance of US Surveillance Laws and Practices with EU Law

I. The standards: Fundamental rights and freedoms guaranteed within the European Union

On October 6, 2015, the Court of Justice of the European Union ("CJEU") issued a judgment in the case of *Schrems v. Data Protection Commissioner* (C-362/14) determining that Commission Decision 2000/520 was invalid. The latter decision, commonly known as the "Safe Harbour Agreement," had found that the United States provided an "adequate level of protection" for personal data for the purposes of Directive 95/46, such that it was lawful for such data to be transferred from the European Union to entities in the US.[2]

In *Schrems*, the Court set out several of the protections that are guaranteed in the EU legal order under the Charter of Fundamental Rights, as previously identified in the Court's case law. According to the Court, it is this "level of protection" to which the protections found in a third country such as the United States must be "essentially equivalent."[3]

The protections guaranteed under the Charter, as set out in *Schrems*, include:

- The existence of "clear and precise rules governing the scope and application of a measure" that interferes with fundamental rights in this area.[4]
- The imposition of "minimum safeguards" such that "the persons whose personal data is concerned have sufficient guarantees enabling their data to be protected against the risk of abuse and against any unlawful access and use of that data."[5]
- The barring of "derogations and limitations in relation to the protection of personal data" except where these are "strictly necessary."[6]

The Court went on to specify that laws permitting limitations on fundamental rights in this context do not meet the requirement of strict necessity where they:

- Fail to provide "an objective criterion" for determining the circumstances under which public authorities may gain access to and use the personal data that has been transferred.[7]

---

[2] Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000D0520&from=EN.

[3] *Schrems v. Data Protection Commissioner*, ¶ 96. In this respect, we disagree with suggestions that the domestic legal orders and surveillance practices of individual EU Member States are relevant to the analysis. See, e.g., Sidley Austin LLP, ESSENTIALLY EQUIVALENT (2016), pp. 33 et seq.

[4] *Schrems*, *supra* n. 3, ¶ 91. Based on the jurisprudence of the European Court of Human Rights, we submit that these rules must be set out in a binding instrument (as distinct from mere policy): see, e.g., *Malone v. United Kingdom*, App. no. 8691/79, Judgment (Plenary), Aug. 2, 1984, ¶¶ 67-68, 87; *Shimovolos v. Russia*, App. no. 30194/09, Judgment, June 21, 2011, ¶ 68 (describing "minimum safeguards [that] should be set out in statute law").

[5] *Id.*

[6] *Id.* at ¶ 92.

[7] *Id.* at ¶ 93.

- Fail to ensure that any such access to and/or use of the data is only carried out for "purposes which are specific, strictly restricted and capable of justifying the interference."[8]
- Permit public authorities "to have access on a generalized basis to the content of electronic communications." According to the Court, such a shortcoming "compromis[es] the essence of the fundamental right to respect for private life" as enshrined in the Charter.[9]
- Fail to "provid[e] for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data." The Court stated that such a situation "does not respect the essence of the fundamental right to effective judicial protection" found in the Charter.[10]

As the Court identified these criteria based on the interpretations of the Charter found in its case law, there is no indication that the adoption of the General Data Protection Regulation (which will repeal and replace Directive 95/46) has altered them. These standards are also generally reflective of those identified by the European Court of Human Rights.[11]

In addition to *Schrems*, the Court has now issued its judgment in the joined cases of *Tele2 Sverige AB v. Post- och telestyrelsen* (C-203/15) and *Secretary of State for the Home Department v. Watson and others* (C-698/15). In that judgment, the Court gave a further indication of the restrictions legislation must impose on access to retained data in order to comply with the Charter of Fundamental Rights:

- Where the legislation permits access to retained data "in relation to the objective of fighting crime," the authorities "as a general rule" should be granted such access "only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime." While exceptional circumstances may exist, for example where "vital national security, defence or public security interests are threatened by terrorist activities," the Court suggested that there should still be "objective evidence from which it can be deduced that the data might, in a specific case, make an effective contribution to combating such activities."[12]
- Except in "cases of validly established urgency," the legislation must ensure that public authorities' access to retained data is "subject to a prior review carried out either by a court or by an independent administrative body" based on a "reasoned request" by the authorities.[13]

---

[8] *Id.*
[9] *Id.* at ¶ 94.
[10] *Id.* at ¶ 95.
[11] See especially *Zakharov v. Russia*, App. no. 47143/06, Judgment (Grand Chamber), Dec. 4, 2015; *Klass and others v. Germany*, App. no. 5029/71, Judgment (Plenary), Sept. 6, 1978; *Szabó and Vissy v. Hungary*, App. no. 37138/14, Judgment, Jan. 12, 2016; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, App. no. 62540/00, Judgment, June 28, 2007; *Shimovolos*, *supra* n. 4.
[12] *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Watson and others*, ¶ 119.
[13] *Id.* at ¶ 120.

- The authorities who have been granted access to the retained data "must notify the persons affected … as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities." Notification, the Court said, is necessary for individuals to enjoy their right to a remedy for abuses of their rights.[14]

The Court also offered a reminder that EU law may provide protections that are "more extensive" than those found in the Convention for the Protection of Human Rights and Fundamental Freedoms (commonly known as the European Convention on Human Rights).[15]

II. Non-compliance of US surveillance laws and practices with these standards

At least two of the United States' most important surveillance authorities, and the programs the country avowedly or reportedly conducts under them, demonstrably fall far short of "essential equivalence" to the standards set out above. We are also concerned about the lack of safeguards applicable to intelligence-sharing arrangements.

As a preliminary matter, we observe that the US government does not regard the protections of the US Constitution, which prohibits "unreasonable" searches and seizures and imposes a warrant requirement to prevent such actions, as extending to non-US persons who are outside the United States.[16] ("United States person" is a term of art that includes US citizens, lawful permanent residents, and some legal persons.)[17] Thus, at least in the intelligence surveillance context, people in the EU who are not US persons will not benefit from these constitutional protections.[18]

a. Executive Order 12333

Originally issued by the executive branch in 1981 and subsequently amended, Executive Order 12333 ("EO 12333") governs the US intelligence agencies' activities (including, but not limited to, electronic surveillance).[19] The order imposes certain broad restrictions concerning the surveillance of US persons' communications under it; however, it appears to grant free rein to

[14] *Id.* at ¶ 121.
[15] *Id.* at ¶ 129.
[16] See, e.g., Answering Brief of Plaintiff-Appellee, *United States v. Mohamud* (9th Cir.), Dec. 7, 2015, p. 101 ("Because the Fourth Amendment generally does not protect non-U.S. persons outside the United States, at least where such persons lack 'substantial connections' to this country, the Fourth Amendment does not prevent the government from subjecting them to warrantless surveillance" (citing *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), in which the US Supreme Court found that the Fourth Amendment does not apply to "the search and seizure by United States agents of property that is owned by a nonresident alien and located in a foreign country")), available at https://www.aclu.org/legal-document/us-v-mohamud-government-response-brief.
[17] 50 U.S.C. § 1801(i).
[18] There are some circumstances in which the Foreign Intelligence Surveillance Act requires US authorities to obtain a warrant from the Foreign Intelligence Surveillance Court before conducting targeted intelligence surveillance of non-US persons, but this is a statutory requirement rather than a constitutional one (see 50 U.S.C. § 1804) and does not constrain the separate surveillance laws and practices described in this letter (for example, the surveillance conducted under Section 702 of FISA).
[19] Executive Order 12333: United States Intelligence Activities (as amended), available at https://fas.org/irp/offdocs/eo/eo-12333-2008.pdf.

the agencies to conduct surveillance overseas of the communications of non-US persons who are outside the US.[20]

Most of EO 12333 has not been codified in statutory law, and the legislature had no role in the order's adoption. In November 2013, the then-chair of the US Senate Select Committee on Intelligence suggested that the US Congress also plays little or no role in overseeing surveillance that takes place under this authority, and there appear to have been no public reports of any change in this respect.[21] Additionally, surveillance under the order is not subject to judicial authorization or oversight, and the government reportedly believes it is not required to notify any individual—including a criminal defendant—that his or her communications have been surveilled under this authority.[22]

Numerous media reports indicate that the US has used EO 12333 as the basis for vast surveillance programs around the world that have involved, among other actions:

- The interception of hundreds of millions of text messages and billions of mobile telephone location updates every day;
- The interception of large quantities of data, including the content of communications, as it was being transmitted between non-US data centers belonging to major internet companies; and
- The acquisition of records of all telephone calls in five foreign states, and the acquisition of the content of those conversations in two of those states.[23]

Thus, EO 12333 surveillance fails to meet several of the standards set out in the CJEU's case-law:

- The measure does not "lay down clear and precise rules governing the scope and application" of the surveillance activities that take place under it, particularly of non-US persons.[24]
- The existing safeguards against abuse are unclear and do not include meaningful congressional or judicial oversight.[25]

---

[20] *Id.* at § 2.3. While EO 12333 can be read to suggest that US intelligence agencies are primarily intended to use surveillance under the order to acquire information "for foreign intelligence and counterintelligence purposes," and while Presidential Policy Directive 28 (see below) currently appears to impose such a stricture, we are not aware of any independently enforceable requirement to this effect. The order also defines the term "foreign intelligence" to include, *inter alia*, "information relating to the capabilities, intentions, or activities of … foreign persons" (§ 3.5(e)). It is difficult to imagine meaningful correspondence by non-US persons that might not meet this definition.

[21] Ali Watkins, "Most of NSA's data collection authorized by order Ronald Reagan issued," MCCLATCHY, Nov. 21, 2013, http://www.mcclatchydc.com/news/nation-world/national/national-security/article24759289.html.

[22] Charlie Savage, "Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide," N.Y. TIMES, Aug. 13, 2014, https://mobile.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html.

[23] American Civil Liberties Union & Center for Democracy & Technology, "Secret Surveillance: Five Large-Scale Global Programs," May 2015, https://cdt.org/files/2014/09/cdt-aclu-upr-9152014.pdf.

[24] See *supra* n. 4.

[25] While the government has adopted internal rules that apply to surveillance under EO 12333, these are designed to protect the rights of US persons and contain many exceptions. See, e.g., United States Signals Intelligence Directive SP0018, Jan. 25, 2011, available at

- Particularly given the breadth of the programs the US government has reportedly conducted pursuant to the executive order, it has not been established that the interference with personal data is limited to what is strictly necessary to achieve a legitimate objective. There is also no existing legal requirement to this effect.
- The government appears to believe it may store and have access to personal data, including the content of communications, on a generalized basis under this authority.
- Access to any retained data is not subject to prior independent review and is not followed by any notification of the individuals affected. The lack of notification, in turn, prevents individuals from having meaningful access to an effective remedy for any abuses (see below).

When assessing the nature and strength of restrictions the US applies in this area, the Commission should take account of the fact that US officials may use an idiosyncratic definition of "collect." For example, one of the main policies applying to US intelligence surveillance provides that "[c]ollection means intentional tasking or [selection] of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record"; we understand this to mean that the government often considers communications to have been "collected" only if an analyst has examined them or otherwise processed them in some way.[26] It follows that the government likely considers it may acquire vast stores of digital information without running afoul of the already limited safeguards against arbitrary "collection" of such information in US law, widening the considerable gap between US practice and the standards set out by the CJEU.[27]

b. Section 702 of the Foreign Intelligence Surveillance Act

Adopted by Congress in 2008, Section 702 of the Foreign Intelligence Surveillance Act ("FISA") empowers the intelligence agencies to "target" non-US persons overseas for warrantless telephone or internet monitoring. As confirmed by the Privacy and Civil Liberties Oversight Board ("PCLOB") in a 2014 report, the agencies operate at least two large-scale warrantless surveillance programs pursuant to this provision.[28] One, "upstream" scanning, allegedly involves the automated bulk searching of communications that flow over the internet infrastructure that links the US to the rest of the globe.[29] The other, PRISM, enables the National Security Agency ("NSA")—with the assistance of the Federal Bureau of Investigation ("FBI")—to demand private communications such as e-mails and instant messages from US internet companies

---

https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf (hereinafter "USSID 18"); Procedures for the Availability or Dissemination of Raw Signals Intelligence Information by the National Security Agency Under Section 2.3 of Executive Order 12333 (Raw SIGINT Availability Procedures), Jan. 3, 2017, available at https://www.dni.gov/files/documents/icotr/RawSIGINTGuidelines-as-approved-redacted.pdf.

[26] USSID 18, *supra* n. 25, § 9.2.

[27] This interpretation may also affect how the US government views its obligations under international human rights treaties, since the US government apparently takes the position that it has not interfered with the right to privacy if personal data is acquired and stored in a database, but has not yet been processed by a human being.

[28] Privacy and Civil Liberties Oversight Board, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014), available at https://www.pclob.gov/library/702-Report.pdf (hereinafter "PCLOB Report").

[29] See Ashley Gorski & Patrick Toomey, "Unprecedented and Unlawful: The NSA's 'Upstream' Surveillance," ACLU, Sept. 23, 2016, https://www.aclu.org/blog/speak-freely/unprecedented-and-unlawful-nsas-upstream-surveillance.

without warrants. Documents disclosed by former NSA contractor Edward Snowden beginning in 2013 indicate that these companies include, among others, Google, Apple, Microsoft, and Facebook.[30]

The purposes for which the government may monitor communications under Section 702 are broad and provide a great deal of latitude: the executive branch need only certify that "a significant purpose" of the surveillance is to obtain "foreign intelligence information."[31] The latter term is expansively defined to include, for example, "information with respect to a foreign power or foreign territory that relates to … the conduct of the foreign affairs of the United States."[32]

Surveillance under Section 702 must formally "target" a non-US person outside the United States, such as an EU national in the EU.[33] While the Foreign Intelligence Surveillance Court ("FISC") must annually approve targeting and other procedures that are intended to provide certain protections for US persons,[34] neither the FISC nor any other independent body authorizes or reviews individual targeting decisions. Thus, although the executive branch has sought to portray Section 702 monitoring as "subject to … independent judicial supervision" in materials submitted to the European Commission as part of the Privacy Shield negotiations,[35] we observe that this supervision is limited to the approval of certain procedures rather than specific decisions to obtain or gain access to personal data, and that even those procedures are neither designed nor required as a matter of law to provide protections for non-US persons.

Moreover, though the executive branch claims its acquisition of information is "targeted" because analysts designate "targets" of interest,[36] there appear to be no acknowledged limits to its power to capture communications "incidentally."[37] It has never publicly disclosed any estimates of the number of these "incidentally" monitored communications, and has recently declined to provide the US Congress with figures describing the impact of incidental collection on US persons.[38] However, when the *Washington Post* evaluated a set of 160,000 leaked emails and instant messages the agencies had gathered under Section 702, it found that 90 percent of the account holders to whom the communications belonged were not the "targets" of this

[30] See "NSA slides explain the PRISM data-collection program," WASH. POST, July 10, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.
[31] 50 U.S.C. § 1881a(g)(2)(A)(v).
[32] 50 USC § 1801(e).
[33] 50 USC § 1881a(a)-(b).
[34] 50 USC § 1881a(d)-(e), 50 USC § 1801(h).
[35] Letter from General Counsel Robert Litt, Office of the Director of National Intelligence, Feb. 22, 2016, p. 9, available at https://iapp.org/media/pdf/resource_center/eu_us_privacy_shield_full_text.pdf.pdf.
[36] *Id*.
[37] See, e.g., Brief of Amicus Curiae, United States Foreign Intelligence Surveillance Court, Oct. 16, 2015, p. 11, available at https://www.aclu.org/foia-document/brief-fisc-amicus-curiae-amy-jeffress?redirect=foia-document/brief-amicus-curiae ("The scope of the incidental collection is broad"); Robyn Greene, "It's Not Just Trump. We Are All Victims of 'Incidental Collection'," NEWSWEEK, Mar. 28, 2017, http://www.newsweek.com/its-not-just-trump-we-are-all-victims-incidental-collection-574776.
[38] Human Rights Watch, "Intelligence Agency Dodges Congressional Scrutiny," June 8, 2017, https://www.hrw.org/news/2017/06/08/intelligence-agency-dodges-congressional-scrutiny.

surveillance.[39] PCLOB has described the scope of such "incidental" acquisition as "unknown and potentially large," while an independent *amicus curiae* for the FISC has characterized it as "broad."[40]

After the NSA and FBI have obtained these potentially vast volumes of personal data (again, without any requirement of a suspicion of wrongdoing and without any individualized approval by an independent body), they may disseminate that data to other agencies under a variety of circumstances. For example, the FBI may share the data with other law enforcement bodies if the Bureau believes it "reasonably appears to be foreign intelligence information or is necessary to understand foreign intelligence information or assess its importance," or if it "reasonably appears to be evidence of a crime."[41] The FBI may also gain access to and "query"—that is, search—communications acquired under Section 702 without any court approval or individualized suspicion of wrongdoing.[42]

Despite the apparently large scale of the PRISM program and "upstream" scanning, the government has provided notifications of Section 702 surveillance to individuals in only a handful of instances.[43] The government is legally required to provide such notifications where it intends to "use" or disclose data "obtained or derived from" surveillance in a proceeding; however, it may be employing excessively narrow definitions of "use" and "derived from."[44] As a result, it is possible that even criminal defendants whose liberty is at stake are being deprived of notice of Section 702 surveillance in some cases.[45] Meanwhile, the government is not obligated to provide notice of Section 702 surveillance to individuals who are not "aggrieved persons" in criminal cases or other official proceedings.

In sum, while Section 702 is subject to congressional oversight and offers a veneer of policy-based protections for US persons, it suffers from flaws that render it noncompliant with EU fundamental-rights standards:

---

[39] Barton Gellman et al., "In NSA-intercepted data, those not targeted far outnumber the foreigners who are," WASH. POST, July 5, 2014, available at https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html?tid=a_inl&utm_term=.6fc55f584d8c.

[40] PCLOB Report, *supra* n. 28, p. 9; Brief of Amicus Curiae, United States Foreign Intelligence Surveillance Court, Oct. 16, 2015, p. 11, available at https://www.aclu.org/foia-document/brief-fisc-amicus-curiae-amy-jeffress?redirect=foia-document/brief-amicus-curiae.

[41] Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, Sept. 21, 2016, pp. 31-32, https://www.dni.gov/files/documents/icotr/51117/2016_FBI_Section_702_Minimization_Procedures_Sep_26_2016_part_1_and_part_2_merged.pdf. While the section of the procedures concerning the FBI's dissemination of information that "reasonably appears to be evidence of a crime" only explicitly addresses information concerning US persons, there is nothing to suggest that the bureau would not similarly be able to disseminate such information where it concerns non-US persons.

[42] *Id.* at pp. 11-12.

[43] See Patrick C. Toomey, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance – Again?", *Just Security*, Dec. 11, 2015, https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again.

[44] 50 U.S.C. § 1806(c). The relevant proceedings may include "any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States."

[45] See *supra* n. 43.

- The purposes for which the authorities may conduct the surveillance are broad and not limited to what is strictly necessary to achieve a legitimate objective.
- There are insufficient safeguards to guarantee against abuse. This problem is particularly acute for non-US persons.
- Except in the rare instances in which the government has provided notification of Section 702 surveillance to a criminal defendant in the US, there is very little meaningful possibility "for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data," where the data was acquired under this law. (See below.)
- The authorities appear to interpret the law as permitting generalized access to and searching of communications, including the content thereof, as part of "upstream" monitoring.
- At least where non-US persons are concerned, the authorities interpret the law as permitting generalized access to and searching of communications through dissemination and querying.
- Due to the use of broad standards for the permissible purposes of the surveillance, as well as targeting decisions that are not subject to independent authorization or review, the PRISM program may also potentially be regarded as permitting generalized access to communications, including the content thereof.

Section 702 is scheduled to expire on December 31, 2017 unless Congress renews it. For the reasons explained above, no measure short of the complete repeal of the law will bring this aspect of the US system into line with EU standards. The Commission should be frank about this circumstance in its interactions with Congress and the US executive branch.

c. Presidential Policy Directive 28

The materials the US government has submitted to support its claim that its intelligence surveillance practices respect fundamental rights rely heavily on Presidential Policy Directive 28 ("PPD-28"), which currently applies to the country's signals intelligence activities (subject to an exception for data "temporarily acquired" in bulk to facilitate more "targeted" monitoring; the US has yet to explain the meaning of this loophole—including, for example, how the government interprets and applies it in practice, or how much data is affected).[46]

PPD-28 is not a law and, like EO 12333, is subject to unilateral alteration or revocation by the executive branch at any time. Notwithstanding the protections ostensibly afforded by its provisions, we believe its status as a unilaterally and instantly revocable policy diminish or eliminate its relevance to an examination of whether the United States provides fundamental-rights protections that are essentially equivalent to those established in the EU legal order.

[46] Presidential Policy Directive 28: Signals Intelligence Activities, Jan. 17, 2014, available at https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2014/01/2014sigint.mem_.ppd_.rel_.pdf (hereinafter "PPD-28"). The European Data Protection Supervisor has also expressed concerns about this loophole: Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision, May 30, 2016, p. 8.

PPD-28 also contains several significant loopholes in addition to the one mentioned above. For example, while the directive states that "[t]he United States shall not collect signals intelligence *for the purpose of* suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion" (emphasis added),[47] it does not contain a prohibition on signals intelligence activities that would have this *effect* in a manner that would violate human rights, even if the stated purpose differs.

Similarly, while PPD-28 purports to impose a default retention period of no more than five years for personal information collected through surveillance, it adds the caveat "unless the [Director of National Intelligence] expressly determines that continued retention is in the national security interests of the United States." There is no requirement that such determinations be made on an individualized basis or in accordance with specific criteria, raising the risk that indefinite retention will occur frequently or arbitrarily, for broad categories of data, or even become the norm rather than the exception.

Additionally, while PPD-28 states that surveillance "shall be as tailored as feasible," we observe (as indicated above) that the permissible purposes of US intelligence surveillance are so potentially broad as to call the meaning of this purported restriction into question.[48] We further observe that "as tailored as feasible" appears to be a significantly lower standard than the requirement in EU law (as identified by the CJEU) that limitations to fundamental rights due to surveillance must be "strictly necessary."

PPD-28 also explicitly maintains that the US "must … collect signals intelligence in bulk" in some circumstances. These circumstances are not identified, nor does the policy endeavor to require that bulk collection be "strictly necessary."

d. Intelligence-sharing agreements

EO 12333 allows the Director of National Intelligence to "enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations."[49] These agreements do not require the approval of the legislature.

The executive branch has released certain historic documents concerning an agreement between the US and the United Kingdom,[50] and Snowden disclosed to journalists a memorandum of understanding suggesting that the US shares raw surveillance data with Israel.[51] However, we are unaware of any intelligence-sharing arrangements whose current scope or details the government has made available to the public.

[47] PPD-28, *supra* n. 46, § 1(b).
[48] See *supra* nn. 20, 31-32 and accompanying text.
[49] EO 12333, § 1.4(b)(4)(A).
[50] National Security Agency/Central Security Service, "UKUSA Agreement Release: 1940-1956," May 3, 2016, https://www.nsa.gov/news-features/declassified-documents/ukusa/.
[51] Memorandum of Understanding (MOU) Between the National Security Agency/Central Security Service (NSA/CSS) and the Israeli SIGINT National Unit (ISNU) Pertaining to the Protection of U.S. Persons (undated), available at http://www.statewatch.org/news/2013/sep/nsa-israel-spy-share.pdf.

In a 2014 interview with Human Rights Watch, a senior US intelligence official claimed that the government is permitted to *receive* intelligence concerning US persons from foreign states even in circumstances where it would be illegal for the US to conduct the surveillance itself, although the authorities cannot *request* such intelligence.[52]

More recently, as part of the Senate Select Committee on Intelligence's confirmation hearing for Mike Pompeo, now CIA Director, Senator Ron Wyden stated:

> Absent a specific request from the CIA, a foreign partner, company, organization or individual may nonetheless provide the CIA with the results of extensive cyber operations or other surveillance, including targeted collection against, or bulk collection that includes the communications of U.S. persons. That information could include the communications of U.S. political figures and political activists, leaders of nonprofit organizations, journalists, religious leaders, businesspeople whose interests conflict with those of President Trump, and countless innocent Americans.[53]

While the information provided by the senior intelligence official and Sen. Wyden focuses on US persons, there are no publicly known strictures that would prevent these remarks from being equally accurate with respect to non-US persons.

In light of the nearly complete opacity of US intelligence-sharing arrangements with other states, as well as the apparent lack of oversight by independent bodies, we believe these arrangements manifestly fail to comply with any of the criteria set out in *Schrems*.

e. Lack of an effective remedy for abuses

As described above, the CJEU has repeatedly emphasized the importance of access to legal remedies for abuses in this context. The text of the Charter suggests that the right requires "an effective remedy before a tribunal," while the Grand Chamber in *Schrems* referred to "judicial protection."[54]

In the United States, this right is not meaningfully available in the warrantless intelligence surveillance context for the overwhelming majority of persons of any nationality. The Supreme Court's ruling in *Clapper v. Amnesty International USA* effectively requires specific facts showing that a particular plaintiff has been or will be monitored (in the Court's words, the demonstration of "a threat of certainly impending interception") in order for him or her to establish standing to challenge the legality of a surveillance law or practice.[55] A recent ruling by the Court of Appeals for the Fourth Circuit in *Wikimedia Foundation et al. v. National Security*

---

[52] Human Rights Watch & American Civil Liberties Union, WITH LIBERTY TO MONITOR ALL (2014), available at https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and.

[53] Senate Select Committee on Intelligence, "Questions for the Record: Mike Pompeo" (completed), Jan. 18, 2017, p. 5, https://www.intelligence.senate.gov/sites/default/files/documents/qfr-011217.pdf.

[54] Charter of Fundamental Rights of the European Union, Article 47(1); *Schrems*, *supra* n. 3, ¶ 95.

[55] *Clapper et al. v. Amnesty International USA et al.*, 133 S. Ct. 1138 (2013), available at https://www.supremecourt.gov/opinions/12pdf/11-1025_ihdj.pdf.

Agency/Central Security Service et al. accepted that Wikimedia, partly by virtue of its descriptions of the sheer volume of its international communications and how "upstream" scanning under Section 702 works, has standing to challenge the constitutionality of that law; however, this reasoning is unlikely to apply to most individuals and may yet be overturned on appeal.[56] Since the government does not provide notifications of warrantless intelligence surveillance to affected persons (except, in very rare instances, in criminal prosecutions), and since most are likely to remain unable to establish standing on other grounds, there is essentially no way for the vast majority of individuals to challenge any of the surveillance authorities or programs described above. The Privacy Act, particularly in light of its exemptions for classified and law-enforcement materials, does not cure this defect.

In the materials that have become annexes to the Privacy Shield decision, the US has relied on PCLOB and the recently established Ombudsperson (who reports to the Secretary of State) in claiming that it is able to "address EU individuals' concerns" about the country's surveillance. However, PCLOB's statute does not empower the Board to receive or address complaints about, or provide a remedy (let alone an enforceable one) for, legal or policy violations in individual cases, even when the body is operational.[57] The Ombudsperson is similarly undercut by, among other things, a lack of authority to receive individual complaints directly, an apparent lack of power to compel the intelligence agencies or other entities to provide information, and an inability to offer anything other than a confirmation that "the complaint has been properly investigated" and that either the intelligence agencies have complied with the law or that any "non-compliance has been remedied." (The Ombudsperson is not permitted to disclose the specific nature of any such remedial action, nor does it appear that he or she has the authority to compel the intelligence agencies to change their practices or treat an individual's data in any particular way, e.g., by rectifying or erasing it.[58]) Such non-existent, inaccessible, opaque, and/or non-binding processes are entirely unsatisfactory and bear little resemblance to the operations of anything that could reasonably be regarded as "judicial protection" or a "tribunal."

Thus, we consider that the United States does not provide an effective remedy for fundamental rights violations stemming from its intelligence surveillance activities.

* * *

For the reasons set out above, we conclude that the US surveillance regime renders the Privacy Shield decision invalid.

---

[56] *Wikimedia Foundation et al. v. National Security Agency/Central Security Service et al.*, 4th Cir., No. 15-2560 (May 23, 2017), available at https://www.justsecurity.org/wp-content/uploads/2017/05/Wikimedia-ca4-20170523.pdf.

[57] See 42 U.S.C. § 2000ee, available at https://www.pclob.gov/library/42USC2000ee-PCLOB_Enabling_Statute-2.pdf.

[58] See Annex A: EU-U.S. Privacy Shield Ombudsperson Mechanism, available at https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g.